UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/312,150	05/14/1999	PHILIP J. MIRE	M-7219-US	2203

7590 07/19/2006

DAVID L. McCOMBS
HAYNES and BOONE, LLP
901 MAIN STREET
SUITE 3100
DALLAS,, TX 75202-3789

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/312,150	MIRE, PHILIP J.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,7-12 and 18-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,7-12 and 18-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 24 April 2006.

2. Claims 1, 7-12 and 18-22 are pending in the application.

3. Claims 1, 7-12 and 18-22 have been rejected.

4. Claims 2-6, 13-17 and 23-29 have been cancelled.

Response to Arguments

5. Applicant's arguments with respect to claims 1, 7-12 and 18-22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 7, 8, 12, 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albanese et al U.S. Patent No. 6,002,768 in view of Banker et al U.S. Patent No. 6,005,938.

As to claims 1 and 12, Albanese et al discloses a method for encrypting data, the method comprising:

providing a first data processing system for a first user including the first user's private key and a master private key [column 7, lines 7-28];

providing a second data processing system for a second user including program instructions and the first user's public key and master public key to generate a session key [column 5, lines 14-30], to encrypt

original data using the session key [column 9, lines 37-43], to encrypt the session key with the first user's public key [column 9, lines 37-43], to encrypt the session key with the master public key [column 9, lines 37-43], to generate a first data packet including a session key and encrypted data and to transmit the first data packet to one or more different data processing systems instead of or in addition to the first data processing system [column 9, lines 44-62]; and

the first data processing system receiving the first data packet and including program instructions to decrypt the encrypted session key with the private key of the first user [column 10, lines 10-17], and to decrypt the encrypted data with the session key to recreate the original data [column 10, lines 10-17].

Albanese et al teaches that it is one key included in the data packet, not a plurality of session keys.

Banker et al teaches a packet that contains multiple encrypted session keys used for different services [column 14, lines 1-15].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Albanese et al so that the data packet that was generated would have included a plurality of encrypted session keys and encrypted data. The generating and transmitting of the data packet would have used the user's public key, the session key, the new session key and the master public key. The first data processing system would have received the packet and decrypted one of the encrypted session keys based on the intende3d service with the private key of the user.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Albanese et al by the teaching of Banker et al because it provides a one-to-one correspondence between the session keys and services. So by having numerous session keys, the system is able to avoid replay attacks [column 2 line 52 to column 3 line 2].

As to claims 7 and 18, Albanese et al teaches storing the user's private key on a data storage medium coupled to the destination data processing system [column 8, lines 4-14].

As to claims 8 and 19, Albanese et al teaches storing the master private key on a data storage medium coupled to the destination data processing system [column 7, lines 7-28].

7. Claims 9, 10, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albanese et al U.S. Patent No. 6,002,768 and Banker et al U.S. Patent No. 6,005,938 as applied to claims 1 and 12 above, and further in view of Dillaway et al U.S. Patent No. 5,742,756.

As to claims 9 and 20, the Albanese-Banker combination does not teach retrieving the user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system [figure 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Albanese-Banker combination so that the user's private key is stored on a smart card coupled to the destination node.

The private key is only retrieved when the smart card is inserted into the smart card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Albanese-Banker combination by the teaching of Dillaway because it utilizes a smart card to perform critical cryptography operations. The smart Card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart Card, and required cryptographic operations are performed on the smart Card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

As to claims 10 and 21, the Albanese-Banker combination does not teach retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system [figure 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Albanese-Banker combination so that the master private key is stored on a smart card coupled to the destination node. The master private key is only retrieved when the smart card is inserted into the smart card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Albanese-Banker combination by the teaching of Dillaway because it utilizes a smart card to perform critical cryptography

operations. The smart card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart card, and required cryptographic operations are performed on the smart card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

8. Claims 11 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albanese et al U.S. Patent No. 6,002,768 and Lohstroh et al U.S. Patent No. 5,768,373 as applied to claims 1 and 12 above, and further in view of Kruys U.S. Patent No. 5,555,309.

As to claims 11, 22 and 29, the Albanese-Banker combination does not teach utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

Kruys teaches a plurality of master keys [column 2, lines 56-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Albanese-Banker combination so that there would have been a plurality of public and private master keys to decrypt the encrypted session keys. There would have been multiple session keys so there would have been a public/private master key set to encrypt and decrypt the session keys.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Albanese-Banker combination by the teaching of Kruys because it utilizes master keys, each one of which is unique to a respective domain member, and is arranged to protect the respective member vector key of each domain member [column 3, lines 55-62].

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy
July 11, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100